Expert Report of

Kevin E. Madura
AlixPartners LLP

April 10, 2020

I submit this Report in the below-cited action pursuant to Federal Rule of Civil Procedure 26(a)(2)(B) and the Scheduling Order in this case.

I. BACKGROUND AND QUALIFICATIONS

1. I am a Senior Vice President in the global Cybersecurity practice group at AlixPartners LLP. I have been retained as an expert in the matter of Kleinman v. Wright, Case No. 9:18-cv-80176 by Dr. Craig Wright, the defendant in this action ("Dr. Wright" or "Defendant") and have been asked to provide my opinion regarding certain questions. AlixPartners is being compensated at a rate of $480 per hour for my work in this matter.

2. I hold a Bachelor of Science in Computer Science from the University of Maryland and a Master's in Technology Management from Georgetown University.

3. I have been reading and writing code personally and professionally for over 12 years and am familiar with many different programming languages, specifically including but not limited to C++. I have written code for a variety of clients, including the Department of Defense, International Business Machines (IBM), local political campaigns, a school district, and a public university, among others. My full CV is attached as Exhibit 4.

4. I have substantial experience in computer security as it relates to computer programming, and I have identified hundreds of vulnerabilities in computer code and computer systems during the course of my professional career. Reviewing so much code also affords me an understanding of the knowledge and experience required to successfully create computer software.

5. I hold a Certified Ethical Hacker certification, a technical qualification that demonstrates expertise in identifying vulnerabilities and other technical weaknesses in computer systems, including programming code.

6. Before AlixPartners I was employed at International Business Machines (IBM) in the Federal consulting practice. IBM Federal is often contracted by various agencies of the United States Government to perform activities relating to information and technology management, including programming and other services. During my tenure at IBM in the Cybersecurity & Biometrics practice, I served as a Subject Matter Expert (SME) in the areas of cybersecurity and applied cryptography, engaging in matters related to securing the process of computer program development and information technology architecture. I have worked with both military and civilian agencies, including the Department of Defense, among others. I was also part of the Public Service Blockchain team that

developed computer programs to explore potential applications of blockchain technology with government agencies.

7. At AlixPartners I regularly assist clients with technical investigations, forensic analysis, and other issues that require expertise in applied cryptography, computer programs, and other technical subjects. I regularly speak to law firms and other professional organizations regarding computer security, cryptocurrencies, and their implications for digital forensics.

8. As a result of my skill, experience, training, and education I have expert knowledge in the areas of computer security, computer program development, and applied cryptography as it relates to blockchain technology.

II. QUESTIONS ASKED

For this report I was asked to inspect certain documents and testimony and provide my opinion on whether the decedent, David Kleiman, had the requisite skills and experience to have written the original Bitcoin core software application released in 2009.

III. EVIDENCE REVIEWED

9. The resume and professional certification of David Kleiman and supporting documents, Bates numbered Kimon_00010690 to Kimon_00010697.
10. DECLARATION OF DAVID A KLEIMAN, Bates numbered KLEIMAN_00413115
11. A memorandum from Diane Clark, Human Resources Director for the City of Lake Worth Florida to Susan Stanton, City Manager dated August 19, 2009 discussing David Kleiman's qualifications.
12. The deposition transcripts of Gavin Andresen and Kimon Andreou in this matter.
13. A web archived copy of David Kleiman's professional biography found at: https://web.archive.org/web/20060519093230/http://s-doc.com/company/management.asp
14. Web archived copies of the S-Lok product technical documentation found at: https://web.archive.org/web/20060523010301/http://s-doc.com/medialibrary/other/PDFs/tech_info/slok_tech_overview.pdf and https://web.archive.org/web/20060523010600/http://s-doc.com/medialibrary/other/PDFs/tech_info/sev_sellsheet.pdf, and https://web.archive.org/web/20080828130153/http://www.s-doc.com/products/slok.asp

15. The Bitcoin client application code, documentation and annotations at https://github.com/bitcoin/bitcoin
16. *The Crypto-Currency Bitcoin and its mysterious inventor*, Joshua Davis, The New Yorker, October 3, 2011.
17. *A Structural Analysis of Bitcoin*, Clemens H. Cap, Department of Computer Science, University of Rostock.
18. Dave Kleiman's publications, including:
    - Microsoft Log Parser Toolkit; Syngress Publishing; Contributing Author, ISBN 1-932266-52-6; (Feb 24, 2005).
    - Security Log Management: Identifying Patterns in the Chaos; Syngress Publishing; Contributing Author, ISBN 1-59749-042-3; (Apr 13, 2006).
    - Perfect Passwords: Selection, Protection and Authentication; Syngress Publishing; Technical Editor; ISBN 1-59749-041-5; (Dec 25, 2005).
    - Winternals Defragmentation, Recovery, and Administration Field Guide; Syngress Publishing; Technical Editor; ISBN 1-59749-079-2; (September 4, 2006).
    - CD and DVD Forensics: Technical Editor, ISBN 1-59749-128-4; (March 12, 2007).
    - How to Cheat at Windows System Administration: Contributing Author, ISBN 1-59749-105-5; (September 15, 2006).
    - Enemy at the Water Cooler: Real Life Stories of Insider Threats, Technical Reviewer, ISBN 1-59749-129-2; (January 7, 2007).
    - Rootkits for Dummies: Forensics Advisor; ISBN 978-0-471-91710-6; (January 30, 2007).
    - Windows Forensic Analysis Including DVD Toolkit: Technical Editor, ISBN 1-59749-156-X; (May 8, 2007).The Official CHFI Study Guide (Exam 312-49): Main author, ISBN 1-59749-197-7; (October 8, 2007).
19. Other documents as referenced in the text below.

IV. OPINION

20. The Bitcoin software was first released on January 9, 2009 when version 0.1 was posted on the internet by "Satoshi Nakamoto," the pseudonym used by the code's original author(s). Satoshi also wrote and distributed the original Bitcoin Whitepaper and devised

the first blockchain database or "ledger." Bitcoin version 0.1 is commonly referred to as the "reference implementation."

21. Up to and including version 0.1.5, published on February 4, 2009, it is believed that Satoshi was the primary author of the code. After that time a wider community of programmers became involved and assisted with future development.

22. The software code went through at least 20 additional subsequent revisions up to and including version 0.3.19 which was released on December 12, 2010, before Satoshi Nakamoto retired from the project and turned control of the code over to Gavin Andresen. These initial releases are commonly referred to as the "Satoshi Code."

23. Gavin Andresen continued to be the lead developer on the Bitcoin source code until 2017 (Andresen depo 26:14).

24. By his own admission in public forums Satoshi worked on the original code alone for at least a year and a half before publishing it publicly[1], though he may have shared earlier private versions with at least 3 people who assisted with its review in late 2008.

25. The Satoshi Code was written in the C++ programing language. C++ is an object-oriented programming language that can generate very efficient, very fast programs. However, it is also notorious for being a very difficult programming language to learn and an even more difficult programming language to write. Being an object-oriented language it requires programmers to create and destroy objects constantly. It also has no built-in memory management functionality which is why C++ is known as a "memory unsafe" language. It is up to the programmer to manually take care of memory management to avoid issues such as memory leaks and dangling references which will cause a program to crash or present security vulnerabilities. Writing C++ code that does not exhibit these issues is extremely hard. Most other object-oriented languages abstract memory management by using a mechanism called a garbage collector, therefore taking this manual task out of the hands of the programmer, but not C++. The requirement to constantly be aware of memory allocation and deallocation, to make sure that every object is freed once and only once, and to never keep a pointer to a freed object, makes C++ a much more challenging experience than most every other

[1] See Satoshi Nakamoto (17 November 2008). "Re: Bitcoin P2P e-cash paper 2008-11-17 16:33:04 UTC". Satoshi Nakamoto Institute at https://satoshi.nakamotoinstitute.org/emails/cryptography/15/. Last retrieved April 3, 2020.

programming language. In contrast to most other programming languages, the requirement to manually manage memory allocations and utilize memory pointers requires knowledge of specific programming techniques. These and other features of C++ make it much less programmer-friendly than most other languages and is often criticized by even experienced programmers as being incredibly complex and unwieldly. It is especially unfriendly to those who "know just enough to be dangerous."

26. A review of the original Bitcoin code shows that it was written by somebody with deep expertise and experience in the C++ language. In fact, world renowned C++ coder Gavin Andresen, the lead programmer on the Bitcoin project development team for at least four years, who routinely interacted with Satoshi until he stepped away, and who is intimately aware of Satoshi's code writing skills referred to him as "definitely a top 10 percent programmer" (Andresen depo at 210:3). Naturally it would be expected that someone in the top 10 percent of a field would have extensive experience and background in activities directly related to that field. The expertise demonstrated in the original Bitcoin code goes beyond what is expected by even a typical programmer. Development of bitcoin required a deep fundamental understanding of cryptography as well as advanced knowledge of data structures, programming algorithms, networking, computer hardware, and specialized programming techniques. The expertise required to write C++ code that reflects this knowledge is difficult to attain and would many require years of hands on programming experience and training.

27. Other industry leading programmers have also made similar public assessments. Dan Kaminsky, a leading Internet-security researcher, is famous among hackers for discovering, in 2008, a fundamental flaw in the Internet Domain Name System which would have allowed a skilled coder to take over any Web site. He is also regarded as one of the world's best experts for testing software errors and weaknesses. In July 2011 he dug deeply into the Bitcoin software in an attempt to uncover its weaknesses. Kaminsky found none he could exploit. This attempt is recounted in a New Yorker article, in which he was interviewed on the subject by the author, Joshua Davis.

28. In this same article, Kaminsky, after noting that the programming style was dense and inscrutable is quoted as claiming, "the way the whole thing was formatted was insane. Only the most paranoid, painstaking coder in the world could avoid making mistakes." He then went on to proclaim, ""He's a world-class programmer, with a deep

understanding of the C++ programming language. He understands economics, cryptography, and peer-to-peer networking."

29. David Kleiman had experience in computer forensics with a specific background in Windows operating system security and electronic discovery for litigation support. None of the information regarding the professional or personal life of David Kleiman shows that he was a skilled programmer in any language, let alone an advanced language such as C++, nor even a novice C++ programmer. His background and certifications show familiarity with utilizing tools that are programmed by others and then analyzing the data produced by those programs. Developing the bitcoin software requires an entirely different set of skills than the ones listed in the documents reviewed for David's background.

30. I have reviewed David Kleiman's resume and professional certification produced as Bates numbers Kimon_00010690 to Kimon_00010697. That resume shows that he was self-employed as a computer forensic investigator from 1997 until his death in 2013. This work entailed assisting legal counsel and their clients in legal disputes and investigations to recreate and opine on facts gleaned from digital evidence. Much of the experience described is managerial and supervisory in nature, and none includes any computer programming in any language at all. Many of the tools involved with computer forensics are driven by user interfaces and do not require advanced knowledge of the underlying programming language in order to extract forensic information. For example, in a report submitted to a Palm Beach court he details a forensic examination performed in the matter of Lighthouse Investment Partners v. Stacey Tenen. In it, Kleiman says he specializes in "computer forensics, data security, and analysis." (Exhibit 1, page 1) Nowhere in the report does he make reference to, or demonstrate experience in, topics related to computer programming or C++.

31. David Kleiman also worked as the Chief Information Security Officer for a software company called Securit-e-doc, Inc. for several years in early the 2000's. I have reviewed the professional biography included in an archived copy of the company's website which is attached as Exhibit 2 to this report. That biography describes the work he undertook at Securit-e-doc as also including a role as product manager for the S-Lok product. In this role his work is describes as "supervis[ing] the development of our Windows operating system lockdown tool…." This description is consistent with the deposition testimony of Kimon Andreou, a colleague of David Kleiman, who worked with him at

Securit-e-doc and wrote the code for the product. (Andreou depo at 16:14). Mr. Andreou also testified that David Kleiman did not know how to write any complex code beyond simple scripts and "needed help many times on creating a simple program". (Andreou depo at 57:5-6). Andreou, who worked closely with Kleiman during their time at Securit-e-doc, states that Kleiman was "not a programmer" (Andreou depo at 9:19). In fact, the main product was developed by Andreou taking David's logic to "put in a program" to automate certain administration tasks. (Andreou depo at 9:14-15).

32. According to documentation from the archived Securit-e-doc website, the S-Lok product was a security administration tool used to secure networked Windows servers. The product was only available commercially for a few years before the company closed down. The S-Lok product enabled system administrators to set certain configuration settings on Windows servers in alignment with security guidelines offered by industry leaders such as Microsoft. A configuration setting allows users of a program (or operating system) to specify conditions or values that are then acted upon by the program. Knowledge of specific configuration settings, such as the ones offered by S-Lok, does not require the requisite knowledge of the underlying program language.

33. David Kleiman also worked for one year as the Vice President of Technical Operations for a small startup company called Intelliswitch. According to his resume, he oversaw the development of a voice-over-IP telephone network, maintained internet services, and provided other IT management for the company. None of this work describes computer programming or C++ language skills.

34. Prior to 1997 David Kleiman worked for three years as the Director of IT for a large construction company maintaining and securing their network infrastructure, and three years as a police officer for the Palm Beach police force where he also had some IT administration duties. He also spent time in the Army in Aviation Logistics. None of the roles included work as a computer programmer or coding in C++.

35. David Kleiman also lists 10 publications on his resume. A review of these publications shows that for more than half of these his role was simply providing technical review and or technical editing for the primary authors. In one publication he served as a "forensic advisor." In three others Kleiman was a co-author, in one case only writing one section of the book. The publications focus primarily on how to utilize existing popular tools to administer computer systems, review log data, or collect forensic information. None of

these publications discuss or cover C++ programming and none of the work effort of David Kleiman on these publications included programming skills in C++.

36. David Kleiman also listed eleven professional certifications in his resume and various professional biographies that were reviewed. These include six certifications relating to systems security, one on system engineering, one on anti-terrorism, and three relating to computer forensics (evidence collection, examination and handling). None of these certifications relate to computer programming nor experience in C++. Many of the certifications demonstrate proficiency in the ability to use pre-packaged tools in the course of forensic investigations. Others are focused exclusively on non-technical skills such as management. In his deposition testimony, his close friend and colleague Kimon Andreou, also stated that Dave Kleiman was very proud of his certifications and liked to collect as many as he could. (Andreou depo at 16:1). Given this, it is reasonable to assume that he would have also listed any credentials, training or certification related to computer programming if he had them. None of the certifications listed require knowledge or experience in advanced C++ programming as part of the certification process.

37. David Kleiman also lists eleven professional affiliations on his resume. Again these all relate to organizations for computer forensics and security professionals and do not require demonstrating proficiency with any programming language as a requirement for membership. He lists no affiliations relating to computer programmers or C++ coding.

38. Between 1983 and 1992 David Kleiman attended courses at four different institutions which are also listed on his resume. He did not earn any college undergraduate or graduate degrees. None of the course work listed includes any relating to computer programming or C++ coding.

39. I also reviewed the biographical information and service offerings from archived versions of Dave Kleiman's website at DaveKleiman.com. This website was used for his computer forensics business which he ran from 1997 until his death. The archive reviewed was from May 30, 2009. This would have been during the same period that Satoshi Nakamoto was busy revising the early versions of the Bitcoin Software. The descriptions of Dave Kleiman's background and experience and the services he offered to provide on his website are consistent with the experience and skills described above. They focused on computer forensic services for litigation support and computer security consulting services. Nowhere on the site was there any mention of computer

programming services or experience, Bitcoin, or C++ coding, in any form. There are also no references to any code repositories, links to programs created by Kleiman, or any other indication that programming was an activity that Kleiman performed on a regular basis. Further, nothing in Kleiman's background would indicate a deep understanding of economics, a key piece noted by Dan Kaminsky in the assessment of original Bitcoin code. The pages viewed are attached to this report as Exhibit 3.

40. It is my understanding that Dave Kleiman suffered significant financial difficulties in the last few years of his lifetime. At times he "would be behind on his mortgage payments" so much that he feared foreclosure and his utility bills were in arrears, among other issues (Andreou Depo 18:7, 26:13). The average salary in 2013 for a person with top-class C++ programming skill as are exhibited by Satoshi Nakamoto, was well in excess of $100,000.[2] Top C++ coders were in very high demand at that time and to this day are considered to be well compensated.

41. Based on all the above information, it is my opinion that the development of the Satoshi Code for the Bitcoin software by Dave Kleiman would be highly inconsistent with his skills and experience.

V. RESERVATIONS

I reserve all rights to modify or supplement this Report if I become aware of any errors or misstatements, or if I become aware of other data or other evidence relevant to my position.

I also reserve all rights to respond to any statements made by the Plaintiffs, witnesses or expert witnesses to which a response is appropriate.

I understand that several depositions remain to be taken in this matter. I may also modify or supplement my opinions in view of opinions or arguments made by any person, including Plaintiffs' counsel and anyone engaged by Plaintiffs to provide opinions.

I may also modify or supplement my opinions if the Court provides litigants with any pertinent additional rulings.

I may expand or modify my opinions as my investigation and study continues and supplement my opinions in light of any relevant orders from the Court or in response to any additional information I review, and matters the Plaintiffs raise, or any opinions Plaintiffs' experts may provide.

[2] See, https://www.glassdoor.com/Salaries/software-engineer-c-developer-salary-SRCH_KO0,29.htm

If called to testify at trial or a hearing in this case, I may use documents and/or materials to help me explain my points and opinions. I may also prepare and use graphics, images, photographs, video recordings, animations, and other presentation aids to help me explain my points and opinions. I may also use images, photographs, graphics, animations, and other presentation aids prepared by other witnesses to help me explain my points and opinions.

Dated: 10 April 2020, Washington, DC

By:

Kevin Madura

EXHIBIT 1

IN THE CIRCUIT COURT OF THE 15TH
JUDICIAL CIRCUIT IN AND FOR PALM
BEACH COUNTY, FLORIDA

Case No.:50 2012CA017723XXXXMB AB

LIGHTHOUSE INVESTMENT
PARTNERS, LLC, a Delaware
Limited Liability Company,

Plaintiff,

v.

STACEY TENEN,

Defendant.
______________________________/

DECLARATION OF DAVID A KLEIMAN

STATE OF FLORIDA)
)
COUNTY OF PALM BEACH)

I, David Kleiman, being of the age of majority, sound mind, and being familiar with the factual matters set forth below, state and affirm as follows:

1. I am a recognized computer security expert who has worked in the Information Technology sector since 1990. I specialize in computer forensics, data security, and analysis. I have been accepted to testify as a computer expert witness in the United States federal courts,

Florida state courts, and United States military courts. I have also served as a court-appointed neutral expert on computer forensic matters. I am a former Florida Certified Law Enforcement Officer, and I have assisted law enforcement agencies in computer crime analysis. Additionally, I am a published author on the subjects of information security and computer forensics.

2. I am one of fewer than 100 Microsoft Windows Enterprise Security - Most Valuable Professionals (MVP) worldwide. Additionally, I hold the following relevant industry certifications: Certified Information Systems Security Professional (CISSP), Certified Electronic Evidence Collection Specialist (CEECS), Digital Forensic Certified Practitioner (DFCP), Certified Computer Examiner (CCE), Certified Data Recovery Expert (CDRE), Certified Information Forensics Investigator (CIFI), and Microsoft Certified Systems Engineer (MCSE).

3. A copy of my Curriculum Vitae is attached hereto and annexed as Exhibit A.

4. I have been retained by the Plaintiff to conduct a forensic examination of their computer systems in relation to an incident that occurred on or about September 18, 2012.

5. I have reviewed the Plaintiff's Complaint for Injunctive Relief and its associated Exhibits. In addition, I have also reviewed the Affidavit of the Defendant Stacey Tenen.

6. The Plaintiff informed me that an intruder using the email address G33ky@att.net and Internet Protocol (IP) address 108.224.166.25 changed the Plaintiff's remote access, LogMeIn, account that was formerly active under the Plaintiff's company account Stacey.tenen@lighthousepartners.com. Stacey Tenen was an Information Technology employee of Lighthouse partners who was terminated on August 31, 2012.

7. An IP address is similar to a phone number as it identifies from where a call, or in this case Internet access, is coming. I performed Internet research of the IP address and it revealed that it is registered to AT&T Internet Services, 2701 N. Central Express way # 2205.15, Richardson, TX 75080 since 2000-06-20 and the records had last been updated on 2010-10-08.

Further, it revealed that this IP address had a canonical name 108-224-166-25.lightspeed.wepbfl.sbcglobal.net. A canonical name is the properly denoted host name of internet connected equipment (computer, cell phone, router etc.). This designation indicates the IP address was routed through SBC Internet Services, Inc. to be designated in use through the systems in West Palm Beach, Florida. This a common use of the AT&T Uverse systems. In IP Address location search showed it to be in the near vicinity of Blue Heron Boulevard, Riviera Beach Florida, near the east of I-95. In was informed the Defendant lived just North of Blue Heron Boulevard and East of I-95. A complete report surrounding my research on IP address 108.224.166.25 is attached hereto and annexed as Exhibit B.

8. LogMeIn.com, 500 Unicorn Park Drive Woburn, MA 01801, is a remote access service that allows you to use access your work computers from a remote location, allowing you to conduct business as if you were local and physically seated at the computer system.

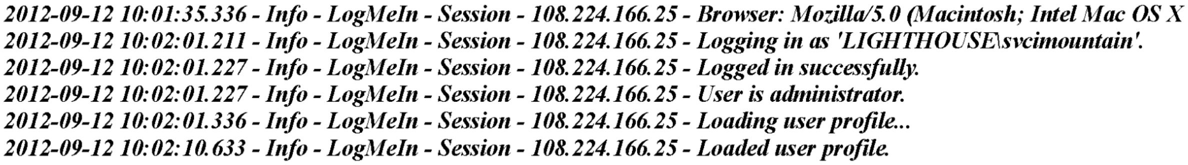
9. On October 01, 2012 through October 04, 2012, I conducted forensic analysis of the Plaintiff's computer systems. The following information is what I have gathered as of October 04, 2012. The examination is ongoing as new evidence has and is being discovered throughout the analysis process.

10. On September 12, 2012 starting on or about 09:48 HRS someone using an Android - Galaxy Nexus and an iPhone utilizing IP address 166.195.242.126 canonical name mobile-166-195-242-126.mycingular.net used LogMeIn to connect to the Plaintiff's computer network. This is indicative of utilizing a cellular broadband connection. It should be noted, that the user utilized known service accounts to then attempt to logon onto Plaintiff's computer systems on the Plaintiff's computer network as noted below.

```
2012-09-12 09:48:57.196 - Info - LogMeIn - Session - 166.195.242.126 - Logging in as 'LIGHTHOUSE\svccentralops'.
2012-09-12 09:48:57.227 - Info - LogMeIn - Session - 166.195.242.126 - Logged in successfully.
```

11. In my experience analyzing network intrusions, this indicates the user had knowledge of these server account names, as there were not dozens, if not hundreds or thousands of failed attempted usernames and passwords before the successful logon as I have seen in my past examinations of outside network intrusions. It should be noted that the LogMeIn log files show there were issues with the systems chosen to attach in this session. One error from the log was "***Unsupported client option: KEYBOARD:IPHONE***".

12. On or about 09:54 IP address 166.195.242.126 logged off from the LogMeIn session. Within minutes, 10:01, another LogMeIn session started from a Macintosh (MAC) computer utilizing IP address 108.224.166.25. Again this intruder immediately logged on to the computer system "**LPPBG1**" a server on the Plaintiff's computer network with a known service account "**SvcImountain**" as noted below.



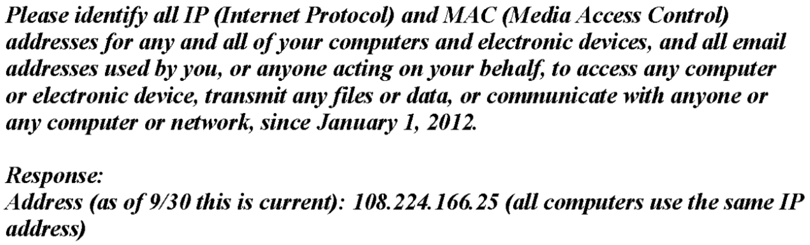
```
2012-09-12 10:01:35.336 - Info - LogMeIn - Session - 108.224.166.25 - Browser: Mozilla/5.0 (Macintosh; Intel Mac OS X
2012-09-12 10:02:01.211 - Info - LogMeIn - Session - 108.224.166.25 - Logging in as 'LIGHTHOUSE\svcimountain'.
2012-09-12 10:02:01.227 - Info - LogMeIn - Session - 108.224.166.25 - Logged in successfully.
2012-09-12 10:02:01.227 - Info - LogMeIn - Session - 108.224.166.25 - User is administrator.
2012-09-12 10:02:01.336 - Info - LogMeIn - Session - 108.224.166.25 - Loading user profile...
2012-09-12 10:02:10.633 - Info - LogMeIn - Session - 108.224.166.25 - Loaded user profile.
```

13. Because the intruder utilized this SvcImountain service account, an account normally reserved for the service, it created a User Profile for that account on the LPPBG1 server. This profile shows a creation date of September, 12, 2012 at 10:02:01, the exact time that the LogMeIn log shows "***2012-09-12 10:02:01.336 - Info - LogMeIn - Session - 108.224.166.25 - Loading user profile...***". A complete printout of the LogMeIn log file from September, 12, 2012 and a screenshot of the SvcImountain profile and its creation date is attached hereto and annexed as Exhibit C

14. I was able to verify by examining the log file output from the Barracuda Firewall utilized by the Plaintiff's on their computer network that IP address 108.224.166.25 had been

utilized by the Defendant Stacey Tenen on August 14, 20102 to VPN into the Plaintiff's computer network system. This was before his termination from employment with Lighthouse Partners. A screen shot of the Barracuda Firewall log file output is attached hereto and annexed as Exhibit D

15. It should be noted that the Defendant stated in his "***DEFENDNT'S ANSWERS TO PLAINTIFF'S FIRST SET OF INTERROGATORIES***" that the 108.224.166.25 was his current (as of September 20, 2012) IP address, and we now from the Barracuda firewall logs that it was his IP address on August 14, 2012.

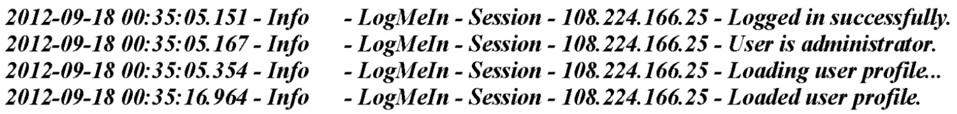


Please identify all IP (Internet Protocol) and MAC (Media Access Control) addresses for any and all of your computers and electronic devices, and all email addresses used by you, or anyone acting on your behalf, to access any computer or electronic device, transmit any files or data, or communicate with anyone or any computer or network, since January 1, 2012.

Response:
Address (as of 9/30 this is current): 108.224.166.25 (all computers use the same IP address)

16. In the Defendants' Affidavit, paragraph 7, Mr. Tenen seems to indicate he only accessed the Palintiff's network computer system on September 18, 2012, but the evidence clearly indicates he accessed the systems on September 12, 2012.

17. On September 18, 2012 starting on or about 00:34 HRS a LogMeIn session started from a Macintosh (MAC) computer, again utilizing the same IP address 108.224.166 to access the Plaintiff's computer network system. Again this intruder immediately logged on to one of the computer server systems "**NTFS17**" a server on the Plaintiff's computer network with the same known service account "**SvcImountain**" as noted below.



```
2012-09-18 00:35:05.151 - Info    - LogMeIn - Session - 108.224.166.25 - Logged in successfully.
2012-09-18 00:35:05.167 - Info    - LogMeIn - Session - 108.224.166.25 - User is administrator.
2012-09-18 00:35:05.354 - Info    - LogMeIn - Session - 108.224.166.25 - Loading user profile...
2012-09-18 00:35:16.964 - Info    - LogMeIn - Session - 108.224.166.25 - Loaded user profile.
```

18. Again, because the intruder utilized a service account to logon to the NTFS17 server, it created a User Profile. This profile shows a creation date of September 18, 2012 at

00:35 hours the exact time the LogMeIn log files shows "***2012-09-18 00:35:05.354 - Info - LogMeIn - Session - 108.224.166.25 - Loading user profile...***" A screenshot of this section of the NTFS17 LogMeIn log file from September, 18, 2012 and a screen shot of the SvcImountain profile on NTFS17 and its creation date is attached hereto and annexed as Exhibit E

19. In the Defendants Affidavit, paragraph 7, Mr. Tenen states "***Following my separation of employment, on September 18,2012, I accessed Lighthouse's server and viewed my human resources file. I started downloading the file and then fell asleep. Sometime later I woke up and reviewed my HR file. When I finished, I then exited the program. I estimate that my computer access time during this LogMeln session, with the breaks and while I fell asleep was approximately 5 hours***" This statement is false. The access on Septmber 18, 2012 shows continued human interaction throughout the four (4) plus hours he was downloading files. Additionally, he did not just download his human resource file, he downloaded thousands of files. Throughout this download time, he picked different directories full of files to download.

i. On or about 00:39 hours he began the File Transfer function and reading searching directories.

ii. At 00:53 hours the first file is downloaded "***E:\HrShared\Administrative Operations and Facilities\Catering\Seamless Service Agreement Lighthouse Investment Partners LLC (LIP 9.6.11).doc (43520 bytes, md5 8630A7176F5AF2C970D4E3CDFDC37DB0)***"

iii. This first File Transfer continues while hundreds of files are downloaded from HRShared directory and its' contents continues until 02:49

iv. At 02:51 the second download begins searching directories and at and 02:54 the one file in this download session "***D:\DATA2\US investors in offshore funds.xls". (93696 bytes, md5 56CB2F59927822D43A2BEAD2AE79B397)***"

v. At 03:04 the third File Transfer session begins and only directories are searched no files are download

vi. At 03:10 the fourth File transfer begins searching directories and at 03;11 the first file is downloaded “"***E:\Data\Users\MAlston\42nd St Freight Elevator Request 5 21 2010.pdf". (62824 bytes, md5 40B9546B4CC241CB4F75D0DC4A363B76)”***

vii. The File Transfer continues and hundreds of files are downloaded and ends at 04:39

20. The above actions indicate human intervention in the starting of each File Transfer session and independently choosing different directories for each File Transfer session. Screenshots of the above mentioned sections from the NTFS17 LogMeIn log file from September, 18, 2012 is attached hereto and annexed as Exhibit F

21. Through his own admission, the defendant has stated he accessed the system on September 18, 2012, although he states in his affidavit “***on September 18, 2012, I accessed Lighthouse's server and viewed my human resources file***”. The evidence shows he downloaded thousands of files. In addition, the defendant accessed at least two other Lighthouse Partner computer network systems on September 18, 2012, the LPPBG1 server at 04:05 , and the CentralOPSNYC server at 03:27 HRS and Screenshots of profiles from LPPBG1 and CentralOPSNYC September, 18, 2012 is attached hereto and annexed as Exhibit G

22. Most alarming is the fact that while he was accessing the systems on September 18, 2012, just a few minutes before he signed off of his remote LogMeIn session, he created a back door account “**Paul Guyot**” with full administrative privileges. Leaving him the option to logon whenever he wanted and it might go unnoticed with just a common username. He then logged onto a workstation “BIGRAT” with the Paul Guyot user account. Further examination is

required to understand the actions done with this user account. Screenshots of some of these accounts activities are attached hereto and annexed as Exhibit H

23. The Defendant tried to cover his tracks by deleting the Microsoft System Event logs. All three of the logs were cleared while the "**SvcImountain**" account was being utilized. During the forensic examination we were able to retrieve the old cleared logs. Both the cleared Security Event log and the new Security Event log contained log entries for the SvcImountain, as well as the System Event log. In fact, the very last entry in the System event log before it was cleared list the user as SvcImountain. The first entry in the Security Event log indicates the Security Audit log was cleared by user SvcImountain, an audit security feature of the Microsoft Security Event log. Screenshots of the Event log activities are attached hereto and annexed as Exhibit I.

24. It is my opinion with a great degree of scientific certainty that the defendant accessed these systems without authorization. In addition, he has accessed and downloaded confidential information and intellectual property. I believe the defendant still has the means, capacity, and mentality to carry out similar unauthorized access to the Plantiff's system.

We arrived at 1000 HRS, the MAC MINI was still in the sealed evidence bag we placed it on 03-Oct-2102. We began disassembling the MAC MINI and immediately began processing the first hard drive. While this was processing we asked about the Lighthouse property and we were informed they were still not completed with their inventory. After an almost 2 hours they finally brought in the property with an inventory list they created and we bean photographing and bagging the evidence items.

1. Item f. paragraph 12 of STenen Affidavit - There was no Bluetooth Keyboard, there was however a Kensington Stylus which was not listed on the Affidavit (see Item 12, Page 3 of our CoC).
2. Item h. paragraph 12 of STenen Affidavit - There were there were no 256GB or 64GB USB drives. However, there were 5 USB Flash/Thumb drives 1 marked 128GB, 2 marked 4GB. the other 2 were not marked, we will report the sizes when we make Forensic images of them (see Item 9, Page 2 of our CoC)
3. Item b. paragraph 12 of STenen Affidavit - There we 18 not 13 iPhones. 14 old 8GB Model A1241s, 2 Model 1303s, 1 32GB 1303B, and 1 Model 1387 (the 4S). It should be noted the 32GB 1303B and the 1387 (4S) were together in the box. Possibly he may have been using the 32GB 1303B along with the 4S (see Items 1-4, Page 1 of our CoC).
4. Not listed on the STenen Affidavit that we did collect was an AT&T 3G MicroCell CSN: 157723526 router (see Item 11, Page 3 of our CoC).

Both hard drives from the MAC MINI were imaged in duplicate (see CFLLC Chain of Custody_2012-09-27_JGreen_Lighthouse_2012-10-11_S.Tenen_MAC-Mini_Signed.pdf).

We placed forensic image drives (Image drive#1 of HD 0, Image drive#1 of HD 1) in evidence bags and noted it as "Maintain custody per STIPULATED ORDER ON PLAINTIFF'S VERIFIED MOTION FOR TEMPORARY INJUNCTION" on the CoC

We placed forensic image drives (Image drive#2 of HD 0, Image drive#2 of HD 1) in evidence bags and noted it as "Maintain custody pending approval of Protocols for Forensic Examination of STenen Computer System" on the CoC, This will be what we pick-up when once the Protocols are agreed upon.

We sealed the MAC MINI in a new evidence bag.

If you would like us to begin forensically preserving Items 3,4,5,6,7,8 and 9 from the Lighthouse Property CoC (CFLLC Chain of Custody_2012-09-27_JGreen_Lighthouse_2012-10-11_Lighthouse_Prop-Pages1-3_Signed.pdf), please advise.

Oct 13-14 2012:

1. Item #3 iPhone model a1303 (iPhone 3GS): This phone is missing the SIM card and appears to be inoperable, therefore no preservation could occur.

2. Item #4 iPhone model A1387 (iPhone 4S): This device was put back into "setup" mode and is missing the SIM card, therefore attempts to extract data met with negative results.

3. Item #5 iPad 64GB model A1430 (iPad 3rd Gen (Wi-Fi/Cellular AT&T/GPS): This device was put back into "setup" mode, therefore attempts to extract data met with negative results. The SIM card was examined and found to contain no useful data.

4. Item #6 ViewSonic ViewPad 7: This device is missing the SIM and memory cards which are need to complete the imaging process.

5. Item #7 Fujitsu Lifebook Model U810: The hard drive was removed and successfully imaged using EnCase software.

6. Item #8 My Book Western Digital EXT HDD: The device successfully imaged using EnCase software. Preliminary observations indicate the was recently formatted on 09/26/12 10:55:27PM and 99% of the 1TB hard drive is unused disk space containing no data (zeros).

7. Item #9 (5 Thumb Drives): The thumb drives were marked 01-05 for identification purpose.
   Drive 01 (128GB diskGO): The device successfully imaged using EnCase software. Preliminary observations indicate the was recently formatted on 09/25/12 12:43:57AM and 99% of the drive is unused disk space containing data.
   Drive 02 (64GB diskGO): The device successfully imaged using EnCase software. Preliminary observations indicate activity on 09/25/12 10:45:38AM when the drive had a folder named "Store-V2" added.
   Drive 03 (128GB diskGO): The device successfully imaged using EnCase software.
   Drive 04 (HP 4GB): The device successfully imaged using EnCase software.
   Drive 05 (HP 4GB): The device successfully imaged using EnCase software.

On Item #7 the newest date was 11/25/11 09:08:27PM

On item #9
03 newest file date was 09/24/12 05:14:17PM
04 newest file date was 01/21/09 03:40:10PM
05 newest file date was 05/22/12 11:06:42AM

Preliminary observations of the MAC Mini show very few files created or modified between 00:00 HRS and 0600 HRS 18-Oct-2012 (see attached spreadsheets). There are no .DOC, .PDF, or XLS files created or modified in the time period. On the spreadsheets highlighted in yellow are information about LogMeIn between 00:48 and 04:45 HRS.

Something I have observed is the Last Written time for the partitions the hard drive in the MAC Mini.

Hard Drive 0 - Volume D - 05-Oct-2012 14:35:54
Hard Drive 0 - Volume 1 Customer - 05-Oct-2012 15:53:05
Hard Drive 1 - Volume 1 Macintosh HD2 - 05-Oct-2012 15:52:14

This could mean the system was being utilized right up until we arrived at the office (unless it was in some sort of hibernation mode). It could also mean the clock on the system is inaccurate, or has been manipulated possibly with the intention of causing confusion in the forensic examination.

Our computer systems are manually updated by the USNO clock at least twice a month, this can be verified via cell phone records.

The first photo was taken of the MAC Mini at approximately 15:35. The box was by itself, no power cables, no monitor, or keyboard, therefore we could not verify the clock accuracy on the MAC Mini. The hard drive was removed and photographed at approximately 16:06. At this time we observed the second hard drive, they asked if we could be done by 17:00, we stated that was an impossibility and put the MAC Mini back together, to return at a later date.

At no time was power applied to this system while in our possession. Hard Drive 0 was not removed until 16:06. We will have to explore the possibilities of how the last write times of 15:53 and 15:52 are on the drive volumes. We will have to check the clock, time zone, and daylight saving settings.

Our examination on the MAC Mini continues.

Examination of the other Lighthouse property:

1. Item #3 iPhone model a1303 (32GB) (iPhone 3GS): This phone is missing the SIM card and appears to be inoperable, therefore no preservation could occur. . We could use a technique were the chip is desoldered from the phone and recover old data directly from the chip, however this is destructive to the phone.

2. Item #4 iPhone model A1387 (iPhone 4S): This device was put back into “setup” mode and is missing the SIM card, therefore attempts to extract data met with negative results. We could use a technique were the chip is desoldered from the phone and recover old data directly from the chip, however this is destructive to the phone.

3. Item #5 iPad 64GB model A1430 (iPad 3rd Gen (Wi-Fi/Cellular AT&T/GPS): This device was put back into “setup” mode, therefore attempts to extract data met with negative results. The SIM card was examined and found to contain no useful data. We could use a technique were the chip is desoldered from the phone and recover old data directly from the chip, however this is destructive to the iPad

4. Item #6 ViewSonic ViewPad 7: This device is missing the SIM and memory cards which are need to complete the imaging process.

5. Item #7 Fujitsu Lifebook Model U810: The hard drive was removed and successfully imaged using EnCase software. The newest file date was 11/25/11 09:08:27PM

6. Item #8 My Book Western Digital EXT HDD: The device successfully imaged using EnCase software. Preliminary observations indicate the was recently formatted on 09/26/12 10:55:27PM and 99% of the 1TB hard drive is unused disk space containing no data (zeros).

7. Item #9 (5 Thumb Drives): The thumb drives were marked 01-05 for identification purpose.

   a. Drive 01 (128GB diskGO): The device successfully imaged using EnCase software. Preliminary observations indicate the was recently formatted on 09/25/12 12:43:57AM and

99% of the drive is unused disk space containing no data. We still have to check the Master Directory Blocks for the actual format date and other factors.

b. Drive 02 (64GB diskGO): The device successfully imaged using EnCase software. Preliminary observations indicate activity on 09/25/12 10:45:38AM when the drive had a folder named "Store-V2" added. We still have to check the Master Directory Blocks to verify the format date and other factors.

c. Drive 03 (128GB diskGO): The device successfully imaged using EnCase software. 03 newest file date was 09/24/12 05:14:17PM (There may be items of evidentiary value on this device)

d. Drive 04 (HP 4GB): The device successfully imaged using EnCase software. 04 newest file date was 01/21/09 03:40:10PM (It seems this device was last used in 2009)

1. 12-Sep-2012 09:48 HRS Accessed the Lighthouse systems utilizing a known Service account and cellular broadband connection IP 166.195.242.126. There were a few errors, this IP logged off at 09:54 HRS. At 10:01 HRS IP address 108.224.166.25 connected through the LogMeIn system to server LPPBG1, with a Macintosh computer, and immediately logged in with a the known Service account SvcImountain

2. 18-Sep-2012 00:34 HRS Accessed the Lighthouse systems connected through the LogMeIn system to server NTFS17 with a Macintosh computer, and immediately logged in with a the known Service account SvcImountain. Was interactively participating in the session that lasted more than 4 hours (04:47 HRS) and downloaded more than 10,000 files. In addition, he accessed at least two othe computer network systems on September 18, 2012, the LPPBG1 server at 04:05, and the CentralOPSNYC server at 03:27 HRS. The Paul Guyot account was created and logged on to workstation BIGRAT at 04:35 HRS.

3. Review of the Mac Mini shows correlation with the NTFS17 LogMein log files:

   a. Created 18-Sep-2012 00:38 HRS com.logmein.LogMeInPluginInstaller.savedState.

   b. Created 18-Sep-2012 04:40 HRS com.logmein.logmeinpluginhost.plist. Contains "rafiletransfer" references.

   c. Created 18-Sep-2012 04:45 HRS com.logmein.ractrlsafari.xml and com.logmein.ractrlsafari.bak.xml.

4. 18-Sep-2012 20:56 HRS the MAC Mini OS on (HD0) is upgraded from 10.8.1 to 10.8.2. LogMeIn logs all indicate it was a MAC with OS 10.8.1

   It should be noted that the MAC Mini has two hard drives and both have Operating Systems (OS) on them. Parallels is installed which is a virtualization software for the MAC, and VMWare Fussion. Similar to VMWare being used at Lighthouse, you can run several Virtual systems on one physical box. Although I found, at least with the current logs, the systems were sued independently. When HD0 was booted HD1 was dormant as an OS, and vice-versa. You could still access the hard drive as secondary drive.

5. 24-Sep-2012 10:20 HRS Received - ltr.spoliation Tenen 092412 Final.pdf in the rootdute@gmail email. The Email was *Starred*.

6. 24-Sep-2012 18:53 HRS Received Summons and Plaintiff's Motion for Temporary Injunction

7. 25-Sep-2012 00:43 HRS (Flash Drive 01) 128GB diskGO drive was formatted. (data still exist in unallocated space on this drive)

8. 25-Sep-2012 10:45 HRS (Flash Drive 02) 64GB diskGO drive activity shown on this drive on the 25th. Unallocated space appears to be zeroed out. This drive was formatted on 04-Sep-2012; one could argue that the unallocated has been zeroed since the format date.

9. 26-Sep-2012 22:55 HRS Book Western Digital EXT 1TB HDD was formatted. Unallocated space appears to be zeroed out.

10. 05-Oct-2012 00:32 HRS according to the System Logs the MAC Mini (HD0) was being utilized and was connected to a volume /Volumes/SSD. The "AFP" messages are showing attempted network connections to the volume named "SSD". This specific entry is a "reconnect" to the volume which could be the user connecting or a "keep alive" type of signal for this network entity. There are other entries all the way up until the SSD Volume is unmounted at 10:20 HRS where this reconnect is occurring on this date as well, and they occur frequently/routinely. I would lean towards more of a "keep alive". All of these are system AFP connections to the SSD volume and not from Time Machine doing an automated mount. The parent process if Time Machine were the trigger would be "com.apple.backupd". Further, I believe these are indicative of the Mac or user "doing something" with this volume. Notice the connection times of "Max reconnect time: 30 secs, Connect timeout: 15 secs for /Volumes/SSD. What this means is when no activity is noted by the Time Capsule, it will disconnect the user. The connection is reestablished when the Mac or user does something with this volume again. In addition, the connections show attempts to mount the volume SSD from the Time Capsule. It is a local network connection as noted by the address //Stac@TimeCapsule._afpovertcp._tcp.local/SSD. There are other entries for the same date for this same network resource.

    It should be noted that the System log for HD0 starts 05-Oct-2012 00:30 HRS. All previous rollover archive logs are missing from the system. Thus, we cannot tell at what time/date the SSD volume was actually connected, to the system.

    a. Oct 5 00:32:31 homebase kernel[0]: AFP_VFS afpfs_DoReconnect started /Volumes/SSD prevTrigger 898 currTrigger 899

    b. Oct 5 00:32:31 homebase kernel[0]: AFP_VFS afpfs_DoReconnect: doing reconnect on /Volumes/SSD

    c. Oct 5 00:32:31 homebase kernel[0]: AFP_VFS afpfs_DoReconnect: posting to KEA EINPROGRESS for /Volumes/SSD

    d. Oct 5 00:32:31 homebase kernel[0]: AFP_VFS afpfs_DoReconnect: Max reconnect time: 30 secs, Connect timeout: 15 secs for /Volumes/SSD

    e. Oct 5 00:32:31 homebase kernel[0]: AFP_VFS afpfs_DoReconnect: connect to the server /Volumes/SSD

    f. Oct 5 00:32:31 homebase.lighthousepartners.com KernelEventAgent[44]: tid 00000000 found 1 filesystem(s) with problem(s)

    g. Oct 5 00:32:32 homebase.lighthousepartners.com KernelEventAgent[44]: tid 00000000 received event(s) VQ_NOTRESP (1)

    h. Oct 5 00:32:32 homebase kernel[0]: AFP_VFS afpfs_DoReconnect: Logging in with uam 13 /Volumes/SSD

i. Oct 5 00:32:32 homebase kernel[0]: AFP_VFS afpfs_DoReconnect: Restoring session /Volumes/SSD

j. Oct 5 00:32:32 homebase kernel[0]: AFP_VFS afpfs_DoReconnect: get the reconnect token

11. 05-Oct-2012 00:58 HRS according to the System Logs there are references to the LogMeIn GUI going online at 00:58 HRS and then offline and online again at 05:58 HRS. However, I also note some references to LogMeIn. These seem to be a part of a daemon/service as they reference going offline/online at 08:38 and 09:38, just shortly after we left court. Although it could have been remotely accessed.

a. Oct 5 00:58:37 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|OFFLINE

b. Oct 5 00:59:05 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|ONLINE

c. Oct 5 05:58:41 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|OFFLINE

d. Oct 5 05:59:08 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|ONLINE

e. Oct 5 08:38:36 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|OFFLINE

f. Oct 5 08:39:05 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|ONLINE

g. Oct 5 09:38:46 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|OFFLINE

h. Oct 5 09:39:11 homebase.lighthousepartners.com LogMeInGUI[22835]: String:WEBSVC|ONLINE

12. 05-Oct-2012 07:30 HRS Motions hearing.

13. 05-Oct-2012 10:20 HRS according to the System Logs Volume SSD is unmounted from the MAC Mini system.

14. 05-Oct-2012 10:36 HRS Oct 5 10:36 according to the System Logs it appears iCloud credentials for Back To My Mac are being turned off.

a. Oct 5 10:36:31 homebase.lighthousepartners.com mDNSResponder[39]: Removing registration domain 10640232.members.btmm.icloud.com.

15. 05-Oct-2012 10:42 HRS according to the System Logs there were modifications to the user "stac" keychain it shows below in paragraph (g.) that the .Me password removed. At 10:45 HRS there are multiple (I only added a few below) modifications This could be addition to info or deletion. The log does not explicitly state what has been modified.

a. Oct 5 10:42:19 homebase.lighthousepartners.com com.apple.SecurityServer[16]: UID 501 authenticated as user stac (UID 501) for right 'system.keychain.modify'

b. Oct 5 10:42:19 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.keychain.modify' by client '/Applications/Utilities/Keychain

Access.app' [27231] for authorization created by '/Applications/Utilities/Keychain Access.app' [27231] (13,0)

c. Oct 5 10:42:19 homebase.lighthousepartners.com coreservicesd[68]: Application App:"Keychain Access" [0x0/0x24c74c5] @ 0x0x7ff4a3d82250 tried to be brought forward, but isn't in fPermittedFrontASNs ((ASN:0x0-0x24c94c7:)), so denying.

d. Oct 5 10:42:19 homebase.lighthousepartners.com WindowServer[163]: [cps/setfront] Failed setting the front application to Keychain Access, psn 0x0-0x24c74c5, securitySessionID=0x186a7, err=-13066

e. Oct 5 10:42:19 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.keychain.modify' by client '/Applications/Utilities/Keychain Access.app' [27231] for authorization created by '/Applications/Utilities/Keychain Access.app' [27231] (100012,0)

f. Oct 5 10:42:50 --- last message repeated 6 times ---

g. Oct 5 10:43:48 homebase.lighthousepartners.com Keychain Access[27231]: Warning: Removed .Me password

h. Oct 5 10:45:00 homebase.lighthousepartners.com com.apple.SecurityServer[16]: UID 501 authenticated as user stac (UID 501) for right 'system.keychain.modify'

i. Oct 5 10:45:00 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.keychain.modify' by client '/Applications/Utilities/Keychain Access.app' [27231] for authorization created by '/Applications/Utilities/Keychain Access.app' [27231] (100013,0)

j. Oct 5 10:45:00 homebase.lighthousepartners.com coreservicesd[68]: Application App:"Keychain Access" [0x0/0x24c74c5] @ 0x0x7ff4a3d82250 tried to be brought forward, but isn't in fPermittedFrontASNs ((ASN:0x0-0x24cd4cb:)), so denying.

k. Oct 5 10:45:00 homebase.lighthousepartners.com WindowServer[163]: [cps/setfront] Failed setting the front application to Keychain Access, psn 0x0-0x24c74c5, securitySessionID=0x186a7, err=-13066

l. Oct 5 10:45:00 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.keychain.modify' by client '/usr/libexec/kcproxy' [27247] for authorization created by '/Applications/Utilities/Keychain Access.app' [27231] (100013,0)

m. Oct 5 10:45:00 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.keychain.modify' by client '/Applications/Utilities/Keychain Access.app' [27231] for authorization created by '/Applications/Utilities/Keychain Access.app' [27231] (100012,0)

n. Oct 5 10:45:12 --- last message repeated 7 times ---

o. Oct 5 10:45:12 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.keychain.modify' by client '/Applications/Utilities/Keychain Access.app' [27231] for authorization created by '/Applications/Utilities/Keychain Access.app' [27231] (100013,0)

16. 05-Oct-2012 10:58 HRS according to the System Logs shows DiskManagement/DiskUtil being utilized and at 11:01 HRS the utility OnyX being run. Although there are legitimate uses for this app, it can be used to remove files and folders, clear information, including browser history, cookies, recent items, and many caches, as well as configure hidden parameters. At 11:02 you can see that credential is successfully created for use stac, and system privilege be successfully authorized to OnyX.app.

a. Oct 5 10:58:27 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'com.apple.DiskManagement.internal.RepairFSCK' by client

'/usr/sbin/diskmanagementd' [27417] for authorization created by '/usr/sbin/diskutil' [27430] (10000B,0)

b. Oct 5 11:01:56 homebase com.apple.launchd.peruser.501[294] ([0x0-0x24eb4e9].com.titanium.OnyX[27382]): Exited: Terminated: 15

c. Oct 5 11:02:19 homebase.lighthousepartners.com com.apple.SecurityServer[16]: checkpw() succeeded, creating credential for user stac

d. Oct 5 11:02:19 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.privilege.admin' by client '/Users/stac/Applications/OnyX.app' [27435] for authorization created by '/Users/stac/Applications/OnyX.app' [27435] (12,0)

e. Oct 5 11:02:19 homebase.lighthousepartners.com com.apple.SecurityServer[16]: Succeeded authorizing right 'system.privilege.admin' by client '/usr/libexec/security_authtrampoline' [27469] for authorization created by '/Users/stac/Applications/OnyX.app' [27435] (3,0)

17. 05-Oct-2012 11:10 HRS according to the System Logs HD1, the second drive and OS in the MAC Mini was booted. Oct 5 11:10:52 localhost bootlog[0]: BOOT_TIME 1349449852 (1349449852 is a Unix Numeric value, when decoded is Fri, 05 October 2012 15:10:52 UTC) A connection to ICloud and a CiscoVPN were enabled.

a. Oct 5 11:11:35 localhost awacsd[222]: Connecting AWACS client: stac,10640232.p01.members.btmm.icloud.com.

b. Oct 5 11:11:35 localhost rpcsvchost[233]: sandbox_init: com.apple.msrpc.netlogon.sb succeeded

c. Oct 5 11:11:36 localhost configd[22]: network configuration changed.

d. Oct 5 11:11:36 homebase configd[22]: setting hostname to "homebase.lighthousepartners.com"

e. Oct 5 11:11:36 homebase mDNSResponder[18]: Adding registration domain 10640232.members.btmm.icloud.com.

f. Oct 5 11:11:38 homebase com.vmware.launchd.vmware[121]: Started network services

g. Oct 5 11:11:38 homebase SystemStarter[349]: Unknown service: CiscoVPN

h. Oct 5 11:11:38 homebase Parallels[355]: Starting Parallels Dispatcher Service

i. Oct 5 11:11:38 homebase Parallels[359]: Parallels Dispatcher Service successfully started

j. Oct 5 11:11:38 homebase prl_naptd[339]: vnic0: DHCP/NAT for 10.211.55.1-10.211.55.254 netmask 255.255.255.0

k. Oct 5 11:11:38 homebase prl_naptd[339]: vnic1: DHCP for 10.37.129.1-10.37.129.254 netmask 255.255.255.0

18. 05-Oct-2012 11:29 HRS according to the System Logs (HD1) shows a reference to the utility OnyX.app. Although there are legitimate uses for this app, it can be used to remove files and folders, clear information, including browser history, cookies, recent items, and many caches, as well as configure hidden parameters. It appears there was an error in correlation to this app. The same reference appears at 11:37 HRS

It should be noted that the system log for HD1 dates back to 17-Sep-2012, yet the only OnyX references are on 05-Oct-2012. All previous rollover archive logs are missing from the system.

a. Oct 5 11:29:06 homebase com.apple.launchd.peruser.501[503] ([0x0-0x5c05c].com.titanium.OnyX[1582]): Exited: Terminated: 15

b. Oct 5 11:29:11 homebase com.apple.launchd[1] (com.apple.collabd.notifications[1596]): Tried to setup shared memory more than once

c. Oct 5 11:29:11 homebase collabd[107]: [CSServiceDispatchHTTPConnection:199 445d60 +0ms] Caught exception "Error executing query [SELECT '{}'::text[], ('a'=>'b')]: ERROR: operator does not exist: unknown => unknown LINE 1: SELECT '{}'::text[], ('a'=>'b')

d. Oct 5 11:37:52 homebase authexec[2034]: executing /System/Library/ScriptingAdditions/StandardAdditions.osax/Contents/MacOS/uid

e. Oct 5 11:37:52 homebase com.apple.launchd.peruser.501[503] ([0x0-0x65065].com.titanium.OnyX[1848]): Exited: Terminated: 15

f. Oct 5 11:37:58 homebase com.apple.launchd[1] (com.apple.collabd.notifications[2042]): Tried to setup shared memory more than once

g. Oct 5 11:37:58 homebase collabd[107]: [CSServiceDispatchHTTPConnection:199 468760 +0ms] Caught exception "Error executing query [SELECT '{}'::text[], ('a'=>'b')]: ERROR: operator does not exist: unknown => unknown LINE 1: SELECT '{}'::text[], ('a'=>'b')

19. 05-Oct-2012 11:40 HRS according to the System Logs HD0, the first drive and OS in the MAC Mini was booted. Oct 5 11:40:59 localhost bootlog[0]: BOOT_TIME 1349451659 (1349451659 is a Unix Numeric value, when decoded is Fri, 05 October 2012 15:40:59 UTC). There are references again to LogMeIn.

a. Oct 5 11:41:15 localhost com.apple.launchd[1] (com.logmein.logmeinserver[66]): open("/Library/Application Support/LogMeIn/log/stdout.log", ...): 2: No such file or directory

b. Oct 5 11:41:15 localhost com.apple.launchd[1] (com.logmein.logmeinserver[66]): open("/Library/Application Support/LogMeIn/log/stderr.log", ...): 2: No such file or directory

c. Oct 5 11:41:53 homebase com.apple.launchd[1] (com.logmein.logmeinguiagentatlogin): Unknown key for boolean: UseLMILaunchAgentFixer

d. Oct 5 11:42:09 homebase com.apple.launchd.peruser.501[271] (com.logmein.logmeingui): Unknown key for boolean: UseLMILaunchAgentFixer

e. Oct 5 11:42:09 homebase com.apple.launchd.peruser.501[271] (com.logmein.logmeinguiagent): Unknown key for boolean: UseLMILaunchAgentFixer

f. Oct 5 11:42:11 homebase.lighthousepartners.com LogMeInGUI[311]: LogMeIn GUI started

g. Oct 5 11:42:14 homebase.lighthousepartners.com LogMeInGUI[311]: Config watcher thread started

h. Oct 5 11:42:14 homebase.lighthousepartners.com LogMeInGUI[311]: remoteControl:INACTIVE

i. Oct 5 11:42:14 homebase.lighthousepartners.com LogMeInGUI[311]: String:RC:INACTIVE

j. Oct 5 11:42:14 homebase.lighthousepartners.com LogMeInGUI[311]: processLine:ACCESSMASK: 18446744073709551615

k. Oct 5 11:42:15 homebase.lighthousepartners.com LogMeInGUI[311]: String:WEBSVC|OFFLINE

l. Oct 5 11:42:37 homebase.lighthousepartners.com LogMeInGUI[311]: String:WEBSVC|ONLINE

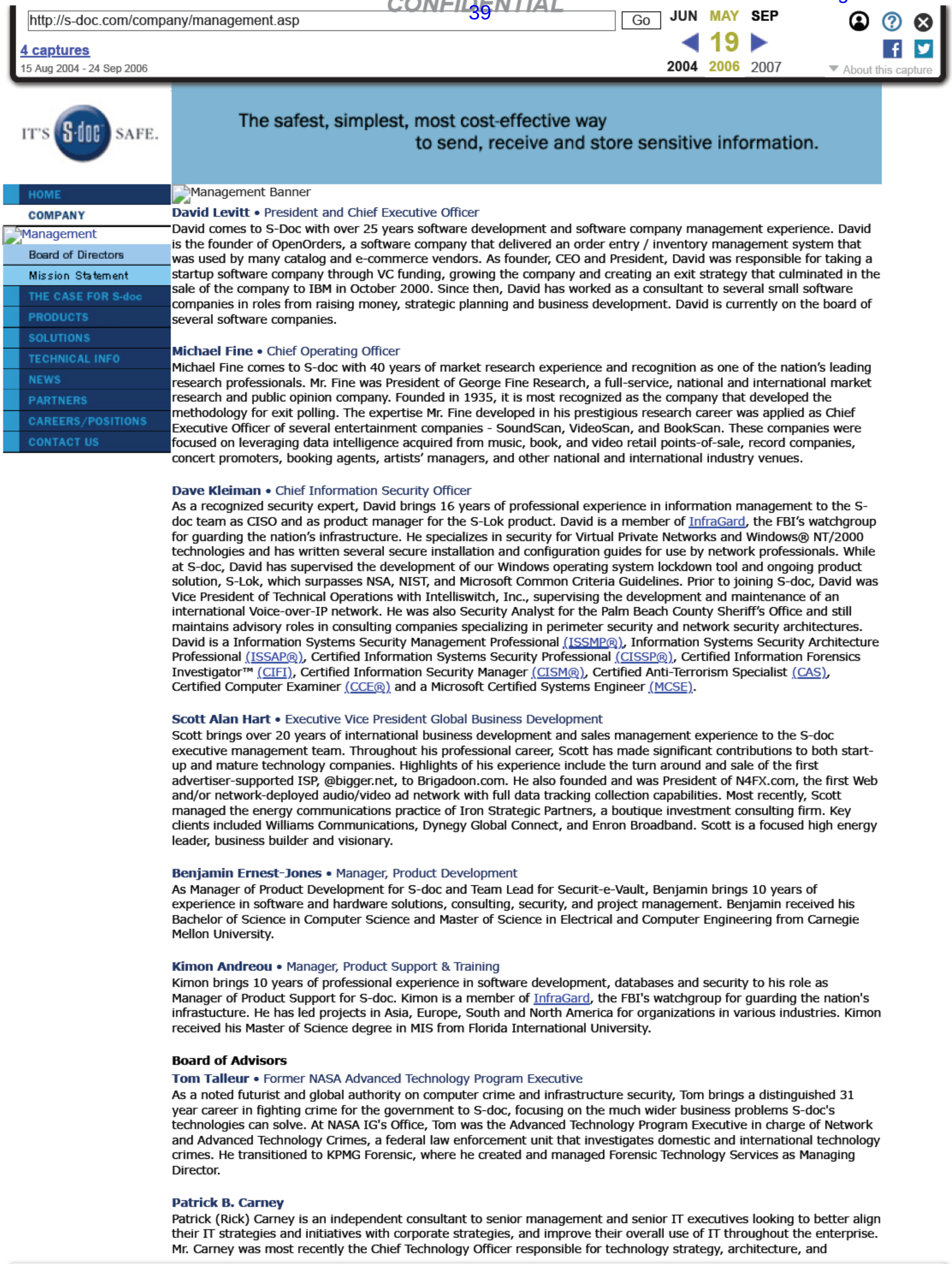
I declare and certify under penalty and perjury under the laws of the United States of America, that the foregoing is true and correct.

Executed on ________________________.

____

David Kleiman, Palm Beach County, Florida

EXHIBIT 2



The safest, simplest, most cost-effective way to send, receive and store sensitive information.

David Levitt • President and Chief Executive Officer

David comes to S-Doc with over 25 years software development and software company management experience. David is the founder of OpenOrders, a software company that delivered an order entry / inventory management system that was used by many catalog and e-commerce vendors. As founder, CEO and President, David was responsible for taking a startup software company through VC funding, growing the company and creating an exit strategy that culminated in the sale of the company to IBM in October 2000. Since then, David has worked as a consultant to several small software companies in roles from raising money, strategic planning and business development. David is currently on the board of several software companies.

Michael Fine • Chief Operating Officer

Michael Fine comes to S-doc with 40 years of market research experience and recognition as one of the nation's leading research professionals. Mr. Fine was President of George Fine Research, a full-service, national and international market research and public opinion company. Founded in 1935, it is most recognized as the company that developed the methodology for exit polling. The expertise Mr. Fine developed in his prestigious research career was applied as Chief Executive Officer of several entertainment companies - SoundScan, VideoScan, and BookScan. These companies were focused on leveraging data intelligence acquired from music, book, and video retail points-of-sale, record companies, concert promoters, booking agents, artists' managers, and other national and international industry venues.

Dave Kleiman • Chief Information Security Officer

As a recognized security expert, David brings 16 years of professional experience in information management to the S-doc team as CISO and as product manager for the S-Lok product. David is a member of InfraGard, the FBI's watchgroup for guarding the nation's infrastructure. He specializes in security for Virtual Private Networks and Windows® NT/2000 technologies and has written several secure installation and configuration guides for use by network professionals. While at S-doc, David has supervised the development of our Windows operating system lockdown tool and ongoing product solution, S-Lok, which surpasses NSA, NIST, and Microsoft Common Criteria Guidelines. Prior to joining S-doc, David was Vice President of Technical Operations with Intelliswitch, Inc., supervising the development and maintenance of an international Voice-over-IP network. He was also Security Analyst for the Palm Beach County Sheriff's Office and still maintains advisory roles in consulting companies specializing in perimeter security and network security architectures. David is a Information Systems Security Management Professional (ISSMP®), Information Systems Security Architecture Professional (ISSAP®), Certified Information Systems Security Professional (CISSP®), Certified Information Forensics Investigator™ (CIFI), Certified Information Security Manager (CISM®), Certified Anti-Terrorism Specialist (CAS), Certified Computer Examiner (CCE®) and a Microsoft Certified Systems Engineer (MCSE).

Scott Alan Hart • Executive Vice President Global Business Development

Scott brings over 20 years of international business development and sales management experience to the S-doc executive management team. Throughout his professional career, Scott has made significant contributions to both start-up and mature technology companies. Highlights of his experience include the turn around and sale of the first advertiser-supported ISP, @bigger.net, to Brigadoon.com. He also founded and was President of N4FX.com, the first Web and/or network-deployed audio/video ad network with full data tracking collection capabilities. Most recently, Scott managed the energy communications practice of Iron Strategic Partners, a boutique investment consulting firm. Key clients included Williams Communications, Dynegy Global Connect, and Enron Broadband. Scott is a focused high energy leader, business builder and visionary.

Benjamin Ernest-Jones • Manager, Product Development

As Manager of Product Development for S-doc and Team Lead for Securit-e-Vault, Benjamin brings 10 years of experience in software and hardware solutions, consulting, security, and project management. Benjamin received his Bachelor of Science in Computer Science and Master of Science in Electrical and Computer Engineering from Carnegie Mellon University.

Kimon Andreou • Manager, Product Support & Training

Kimon brings 10 years of professional experience in software development, databases and security to his role as Manager of Product Support for S-doc. Kimon is a member of InfraGard, the FBI's watchgroup for guarding the nation's infrastucture. He has led projects in Asia, Europe, South and North America for organizations in various industries. Kimon received his Master of Science degree in MIS from Florida International University.

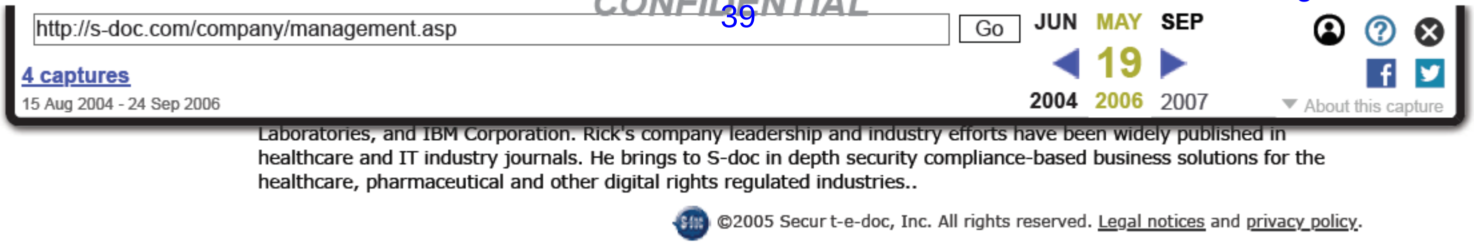
Board of Advisors

Tom Talleur • Former NASA Advanced Technology Program Executive

As a noted futurist and global authority on computer crime and infrastructure security, Tom brings a distinguished 31 year career in fighting crime for the government to S-doc, focusing on the much wider business problems S-doc's technologies can solve. At NASA IG's Office, Tom was the Advanced Technology Program Executive in charge of Network and Advanced Technology Crimes, a federal law enforcement unit that investigates domestic and international technology crimes. He transitioned to KPMG Forensic, where he created and managed Forensic Technology Services as Managing Director.

Patrick B. Carney

Patrick (Rick) Carney is an independent consultant to senior management and senior IT executives looking to better align their IT strategies and initiatives with corporate strategies, and improve their overall use of IT throughout the enterprise. Mr. Carney was most recently the Chief Technology Officer responsible for technology strategy, architecture, and

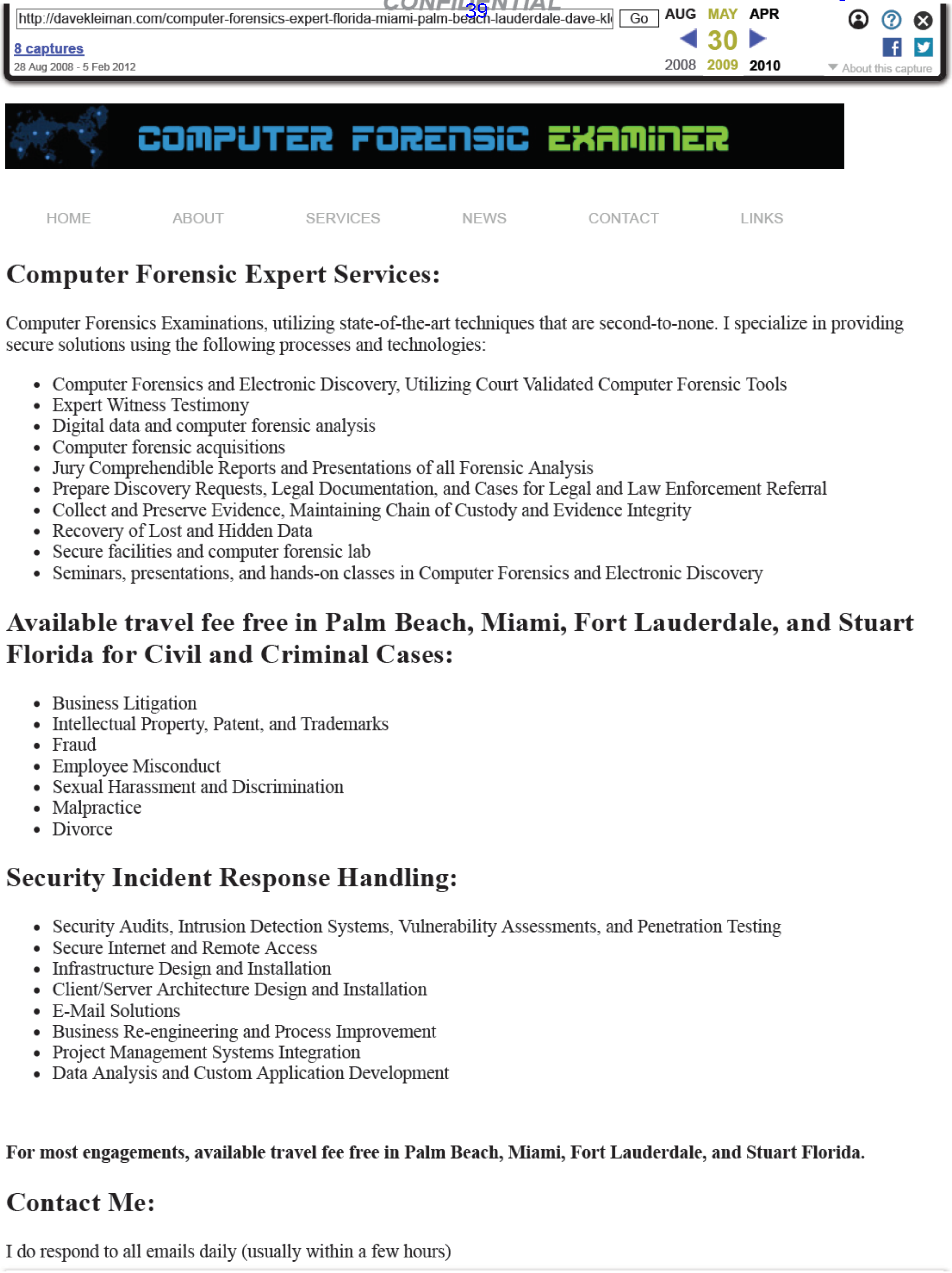


http://s-doc.com/company/management.asp

Laboratories, and IBM Corporation. Rick's company leadership and industry efforts have been widely published in healthcare and IT industry journals. He brings to S-doc in depth security compliance-based business solutions for the healthcare, pharmaceutical and other digital rights regulated industries..

©2005 Secur t-e-doc, Inc. All rights reserved. Legal notices and privacy policy.

EXHIBIT 3


http://davekleiman.com/computer-forensics-expert-florida-miami-palm-beach-lauderdale-dave-kl
Go
AUG MAY APR
30
2008 2009 2010
8 captures
28 Aug 2008 - 5 Feb 2012
About this capture
HOME ABOUT SERVICES NEWS CONTACT LINKS

COMPUTER FORENSIC EXAMINER

Computer Forensic Expert Services:

Computer Forensics Examinations, utilizing state-of-the-art techniques that are second-to-none. I specialize in providing secure solutions using the following processes and technologies:

- Computer Forensics and Electronic Discovery, Utilizing Court Validated Computer Forensic Tools
- Expert Witness Testimony
- Digital data and computer forensic analysis
- Computer forensic acquisitions
- Jury Comprehendible Reports and Presentations of all Forensic Analysis
- Prepare Discovery Requests, Legal Documentation, and Cases for Legal and Law Enforcement Referral
- Collect and Preserve Evidence, Maintaining Chain of Custody and Evidence Integrity
- Recovery of Lost and Hidden Data
- Secure facilities and computer forensic lab
- Seminars, presentations, and hands-on classes in Computer Forensics and Electronic Discovery

Available travel fee free in Palm Beach, Miami, Fort Lauderdale, and Stuart Florida for Civil and Criminal Cases:

- Business Litigation
- Intellectual Property, Patent, and Trademarks
- Fraud
- Employee Misconduct
- Sexual Harassment and Discrimination
- Malpractice
- Divorce

Security Incident Response Handling:

- Security Audits, Intrusion Detection Systems, Vulnerability Assessments, and Penetration Testing
- Secure Internet and Remote Access
- Infrastructure Design and Installation
- Client/Server Architecture Design and Installation
- E-Mail Solutions
- Business Re-engineering and Process Improvement
- Project Management Systems Integration
- Data Analysis and Custom Application Development

For most engagements, available travel fee free in Palm Beach, Miami, Fort Lauderdale, and Stuart Florida.

Contact Me:

I do respond to all emails daily (usually within a few hours) http://davekleiman.com/computer-forensics-expert-florida-miami-palm-beach-lauderdale-dave-kl Go

AUG MAY APR

◀ 30 ▶

2008 2009 2010

8 captures

28 Aug 2008 - 5 Feb 2012

About this capture

4371 Northlake Blvd #314
Palm Beach, Florida 33410
561.310.8801

Computer Forensics can Reveal Important Information:

Your Country Flag is:

Your IP is: 67.202.41.3
Click Here for more IP Address Info

Security News Ticker

symantec.

Security Alerts

Latest Threats

1	05-29-09	Packed.Generic.229
1	05-29-09	Packed.Generic.230
1	05-29-09	Bloodhound.Exploit.241
1	05-29-09	Bloodhound.Exploit.242
		More...

Removal Tools

- Symantec Trojan.Ransomlock Key Generator Tool
- Trojan.Initbar

More...

Security Advisories

- Microsoft PowerPoint Data Out of Bounds Remote Code Execution Vulnerability
- Microsoft PowerPoint File Parsing Remote Code Execution Vulnerability

More...

Search Threat Database

go

www.DigitalComputerForensicExpert.com | www.DaveKleiman.com | www.ComputerForensicExaminer.com

EXHIBIT 4

KEVIN MADURA

Washington, DC | 242-665-2990 | kmadura@alixpartners.com

EDUCATION

University of Maryland
Bachelor of Science, Computer Science; Minor in Leadership Studies **2010-2014**
Awards: Corporate Scholars Scholarship, Order of Omega

Georgetown University
Master of Professional Studies, Technology Management **2015-2017**
Capstone: “Smart Traffic: Controlling Congestion with Technology”

RELATED EXPERIENCE

Independent Research 2009
Discovered a software vulnerability, CVE-2009-0499, which was a “cross-site request forgery (CSRF) vulnerability in the Moodle forum software that allows remote attackers to delete or modify data.”

IBM
Cybersecurity Consultant - Cryptography SME **2014 - 2018**
Provided subject matter expertise in areas of cryptography, secure coding, and vulnerability management for entities within the Department of Defense.

Deployed technical solution to verify identity of soldiers using Common Access Cards (CAC) using cryptographic primitives such as SHA256 and public key cryptography,in alignment with NIST 800-53.

Hosted “lunch & learns” to educate colleagues on secure coding methodologies and case studies.

IBM
Blockchain Identity Expert: Federal Agency **2017**
Primary architect of enterprise identity solution based on blockchain technology, which included validating the proper use of cryptography and secure coding methodology.

IBM
Blockchain Programmer: USPS **2017 - 2018**
Led development of blockchain implementation and smart contract coding for government blockchain pilot programs.

AlixPartners
Senior Vice President, Cybersecurity Practice **2018 -**
Advise clients on cybersecurity matters, ranging from technical implementation issues to executive risk management functions.

Performed forensic investigation for mobile application development company to determine exposure of malicious code and vulnerable software development kits.

Member of blockchain industry team tasked with exploring applications of distributed ledger technology for enterprise clients, implementing cryptocurrency coins, and proper management of Bitcoin wallets.

CERTIFICATIONS

Certified Ethical Hacker
Credential ID ECC39758882107 2018

CONFERENCE PRESENTATIONS

Armed Forces Communications and Electronics Association
Cybersecurity in the World of Blockchain and Cryptocurrency **2018**
A discussion on the applicability of implementing blockchain technology, based on Bitcoin, for use within the US military.

AlixPartners
Procurement Forum **2018**
Explained the potential application of blockchain technology in a business setting to procurement executives at an event hosted by AlixPartners.

Center for Professional Education
Managing Cyber Risk **2018**
Hosted a session focused on managing cyber risks with emerging technologies such as blockchain and cryptocurrencies.

Center for Professional Education
Blockchain & Cryptocurrencies **2019**
A presentation detailing the inner workings of blockchain technology and how Bitcoin spawned thousands of alternative cryptocurrencies.

PUBLICATIONS AND PAPERS

Blockchain 101: What is it?
LinkedIn Article 2017

How Cybersecurity Risk is Disrupting the M&A Landscape
AlixPartners 2019

AWARDS

Corporate Scholars Scholarship	2013
IBM Manager's Choice Award (14)	2016 – 2017
IBM Global Business Services Excellence Award	2017

MEMBERSHIPS

Armed Forces Communications and Electronics Association (Inactive)
EC-Council
Washington DC Cyber Security for Control Systems

TECHNICAL SKILLS

Computer programming languages (C, C#, Go, Java, Bash, Python, Javascript, PHP, Ruby)
Computer systems (Linux, Windows, Mac OS)
Applied cryptography

- Asymmetric encryption (elliptic curve, RSA)
- Symmetric encryption
- Public key infrastructure, X.509 certificate management
- Hashing (HMAC, MD5, SHA family, etc.)
- Transport Layer Security (ciphersuite selection, configuration)

Blockchain analysis

- Personal research reviewing academic papers covering Bitcoin blockchain analysis techniques
- Developed code to parse information from the Bitcoin blockchain
- Study of industry materials, cryptography textbooks (e.g. *Applied Cryptography* by Bruce Schneier)

Secure application coding techniques

- Web application security (OWASP Top 10, SANS Institute best practices)

Vulnerability detection

- Software applications, cryptographic weaknesses, common code vulnerabilities

Computer network security

- Denial of service attack methods, interception/manipulation of traffic, networking protocols (TCP, UDP)

System administration

- Patching methodology, configuration hardening

LANGUAGES

English– native language